Implementering av EU:s direktiv om nät- och informationssäkerhet (NIS)

Bryssel den 5 Juli 2016

VD-SAMMANFATTNING

Den 21 april 2016 publicerade Europeiska Unionens Råd slutversionen av direktivet om nät- och informationssäkerhet (NIS). Även om detta måste undertecknas formellt av Europaparlamentet i sommar, har texten i sig överenskommits av de tre EU-institutionerna och förväntas inte ändras. Medlemsstaterna ska införliva det i sina nationella lagar inom 21 månader efter att det antagits. För att bistå i denna process, läs om god praxis i den medföljande bilagan om hur man implementerar de aspekter som är relevanta för teknikbranschen och vilka på ett effektivt sätt innesluter avtalsutkastförfattarnas intentioner.

EU:s direktiv om nät- och informationssäkerhet är den första paneuropeiska lagen om cybersäkerhet och den fokuserar på att stärka cybermyndigheterna på nationell nivå, vilket ökar samordningen bland dem och inför säkerhetskrav för viktiga branschsektorer.

En nationell genomförandelag ska inte förlora siktet på direktivets två huvudsakliga mål: (1) att garantera en hög nivå på cybersäkerheten i landets avgörande infrastruktur, (2) att etablera en effektiv samarbetsmekanism bland EU:s medlemsstater för att främja detta mål. Resurser ska först och främst användas för att uppnå dessa två viktiga mål.

För teknikbranschen är de bestämmelser som rör de så kallade digitala tjänsteleverantörerna av särskilt intresse. Direktivet anger tydligt att det finns grundläggande skillnader mellan operatörer av nödvändiga tjänster och digitala tjänsteleverantörer. De senare ska verkligen inte anses vara avgörande för infrastrukturen i sig. Precis som lagen anger skulle en incident som påverkar dessa digitala tjänster utgöra en markant mindre risk för ett lands ekonomiska och allmänna säkerhet. Att behålla denna distinktion är avgörande för att även effektivt och faktiskt utnyttja knappa resurser hos myndigheter som kommer att behöva övervaka och driva igenom reglerna.

Därför förespråkar vi en stor uppmärksamhet på den avsedda omfattningen av de berörda tjänsterna och manar beslutsfattare att inte inkludera andra sektorer än de som identifierats som operatörer av nödvändiga tjänster och digitala tjänsteleverantörer för säkerhetskrav i nationell lag.

Med avseende på jurisdiktionen, bör digitala tjänsteleverantörer kunna förlita sig på tillämplig lag i det land där de har sin huvudsakliga etablering, även i fall då behöriga myndigheter från mer än ett land är inblandade. Vid tillsyn, bör behöriga myndigheter följa en efterhandsmetod i stället för att ålägga en allmän skyldighet att övervaka digitala tjänsteleverantörer. Dessutom bör de fokusera på resultat och bibehålla distinktionen mellan operatörer av nödvändiga tjänster och digitala tjänsteleverantörer genom att inte ålägga de senare krav som inte föreskrivs i direktivet, som till exempel anvisningar om revision och bindande instruktioner.

Säkerhetsåtgärder för digitala tjänsteleverantörer bör vara annorlunda än de för operatörer av grundläggande tjänster, mot bakgrund av att direktivets uttalande att dessa representerar en avsevärt lägre säkerhetsrisk. Beslutsfattare bör inse målet med harmonisering för dessa tjänster, erkänna de befintliga branschledda

DIGITALEUROPE
Rue de la Science 14, 1040 Bryssel [Belgien]
Tel: +32 (0) 2 609 53 10 Fax: +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Medlem i kommissionens öppenhetsregister: 64270747023-20

internationella standarderna, undvika tekniska krav och följa de rättigheter som digitala tjänsteleverantörer har i direktivet att definiera de mest lämpliga säkerhetsåtgärderna för sina system. Händelserapporteringen bör även vara så harmoniserad som möjligt på europeisk nivå, bör fokuseras på händelser som påverkar tjänstens kontinuitet, respektera den tidsmässiga flexibiliteten för en anmälan och skapa en tillförlitlig miljö som uppmuntrar informationsdelning utan att utsätta den meddelande parten för ökat ansvar.

De åtgärder som åläggs operatörer av nödvändiga tjänster kommer även att påverka andra branschen då säkerhetsåtgärder och händelserapportering kommer att påverka avtalsbestämmelserna. Detta stämmer särskilt väl för molntjänster. Därför kan digitala tjänsteleverantörer indirekt bli föremål för kundernas nationella lagar och följaktligen har vi ett stort intresse av att se att internationellt erkända säkerhetsåtgärder tillämpas för dessa tjänster. Vi föreslår även samordning och synergieffekter så långt som det är möjligt mellan redovisningskraven för både operatörer av nödvändiga tjänster och för digitala tjänsteleverantörer, då de senare sannolikt blir föremål för dubbel anmälan.

Direktivet anger en ambition att uppnå en hög allmän säkerhetsnivå för nätverk och informationssystem för att förbättra funktionen hos den interna marknaden. För att uppnå detta högtsträvande mål, **bör nationella införlivanden fokusera på en riskbaserad, harmoniserad och internationell metod** som ger aktörer i den privata sektorn flexibiliteten att anpassa sig till en ständigt föränderlig hotbild, möjliggöra cybermyndigheter att rikta de begränsade resurserna till de viktigaste utmaningarna och erkänna att lösningen på ett gränslöst problem måste vara global. Vi hoppas att dessa riktlinjer är ett användbart verktyg i riktning mot detta syfte och svarar gärna på era ytterligare frågor.

DIGITALEUROPE
Rue de la Science 14, 1040 Bryssel [Belgien]
Tel: +32 (0) 2 609 53 10 Fax: +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Medlem i kommissionens öppenhetsregister: 64270747023-20

Bilaga: Riktlinjer för god praxis avseende implementering av nät- och informationsdirektivet

1. Digitala tjänsteleverantörer

a) Omfattning

- Direktivet fastställer att marknadsplatser på internet, sökmotorer på internet och molntjänster ska betraktas som digitala tjänsteleverantörer och följaktligen omfattas av direktivet. Samtidigt som detta direktiv har minimikrav för harmonisering (artikel 2), är det viktigt att vara konsekvent i EU och följaktligen bör medlemsstaterna endast tvinga de sektorer som identifieras som digitala tjänsteleverantörer eller operatörer av nödvändiga tjänster – enligt definitionen i artikel 3 – att följa säkerhetskraven i nationell lag.

- Direktivet anger explicit att maskinvarutillverkare och programvaruutvecklare inte är operatörer av nödvändiga tjänster eller digitala tjänsteleverantörer och följaktligen ska de inte omfattas av de nationella lagar som implementerar direktivet (skäl 50).

- Direktivet utesluter uttryckligen att marknadsplatser på internet ska omfattas, vilka fungerar som mellanhänder till tredjepartstjänster där försäljnings- och serviceavtal slutligen ingås (t.ex. jämförelsesajter) (skäl 15).

- Sökfunktioner begränsade till innehållet på en viss webbplats ska inte definieras som sökmotorer på internet, även om de använder en extern leverantör (skäl 16).

- Definitionen på en molntjänst beror enligt direktivet på om de datorrelaterade resurserna delas av många användare (artikel 4.19 och skäl 17). Eftersom privata moln (i motsats till offentliga moln) är ägnade för en enda organisation, bör de inte omfattas.

- Direktivet understryker att det finns grundläggande skillnader mellan operatörer av nödvändiga tjänster och digitala tjänsteleverantörer, vilket är anledningen till att digitala tjänsteleverantörer är föremål för andra regler (skäl 57). En sådan distinktion bör bibehållas när direktivet implementeras.

b) Domstols behörighet och översikt

- Domstolsbehörigheten för digitala tjänsteleverantörer bör endast förläggas till en medlemsstat, där operatören har din huvudsakliga etablering i EU, vilket i princip motsvarar den plats där denne har sitt säte i EU (artikel 18.1 och skäl 64). Vi hävdar att de digitala tjänsteleverantörerna själva bör fastställa detta och beslutet ska endast vara föremål för granskning om behöriga myndigheter ifrågasätter det i händelse av en efterhandskontroll.

- När digitala tjänsteleverantörer har nätverks- och informationssystem i andra länder än det land där de har sitt säte, förutses det i artikel 17.3 att behöriga myndigheter samarbetar. Ur de digitala tjänsteleverantörernas synvinkel, är det emellertid viktigt att de lagar som tillämpas fortsätter att

utgöras av lagarna i landet där företaget har sitt säte och att de fortsätter att endast ansvara för inför behöriga myndigheter i den jurisdiktionen, som kommer att fungera som företagets samtalspartner.

- I direktivet betonas att digitala tjänsteleverantörer är föremål för återverkande efterhandskontroll. Följaktligen har inte behöriga myndigheter någon allmän skyldighet att kontrollera digitala tjänsteleverantörer och bör endast vidta åtgärder när de förses med bevis. (Artikel 17.1 och skäl 60). Dessa bestämmelser bör följas när direktivet implementeras.

- I motsats till operatörer av grundläggande tjänster, kan myndigheter från digitala tjänsteleverantörer endast utkräva information samt kräva att de digitala tjänsteleverantörerna åtgärdar eventuella fel. Direktivet klargör att myndigheter inte har någon granskningsrätt och inte kan utfärda bindande instruktioner. Dessa bestämmelser bör även följas på nationell nivå.

c) Ytterligare krav

- Digitala tjänsteleverantörers säkerhets- och anmälningskrav är föremål för maximal harmonisering (artikel 16.10). Denna artikel bör övervägas att tillämpas för produkter, tjänster och lösningar som ingår i deras nätverks- och informationssystem. Därför bör ytterligare bestämmelser, som till exempel produkttester, inte utkrävas i den utsträckning som produkterna och tjänsterna används i det sammanhanget.

d) Säkerhetsåtgärder och standarder

- Säkerhetsåtgärderna för digitala tjänsteleverantörer bör vara mildare än de för operatörer av grundläggande tjänster. Digitala tjänsteleverantörer bör fritt kunna definiera hur de arbetar med säkerhet och hur de vill garantera skydd av sina nätverks- och informationssystem och vilka som är lämpliga för de risker som föreligger (skäl 49).

- Säkerhetsåtgärderna bör vara processorienterade och fokusera på riskhantering. Enligt dem bör det inte föreligga krav på att IKT-produkter utformas, utvecklas eller tillverkas på ett visst sätt (skäl 51).

- Direktivet understryker att medlemsstater inte ska införa ytterligare säkerhetskrav på digitala tjänsteleverantörer (artikel 16.10).

- Inte desto mindre förväntar vi oss riktlinjer från ett flertal aktörer. Medlemsstater kommer att garantera att de åtgärder som anges i direktivet tas i bruk (artikel 16.1); de kan uppmuntra till att använda standarder för att implementera dem (artikel 19.1) och diskutera standarderna med europeiska standardiseringsorganisationen i samarbetsgruppen (artikel 11.3 h). Enisa kommer att innehålla råd om lämpliga standarder (artikel 19.2) och EU-kommissionen är ansvarig för att anta genomförandeakter om säkerhetsåtgärderna (artikel 16.8).

- Mot bakgrund av denna komplikationsnivå och nyttan av harmoniseringen, tillråder vi att den nationella processen i huvudsak bör foga sig efter genomförandeakterna avseende samtycke till tillämpliga åtgärder, vilket i varje fall kommer att behövas slutföras inom ett år efter att direktivet antagits. Själva

DIGITALEUROPE
Rue de la Science 14, 1040 Bryssel [Belgien]
Tel: +32 (0) 2 609 53 10 Fax: +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Medlem i kommissionens öppenhetsregister: 64270747023-20

genomförandeakterna bör inte ha någon inverkan på digitala de tjänsteleverantörernas förmåga att definiera de säkerhetsåtgärder som är mest lämpade för sina system.

- Artikeln om standarder möjliggör att europeiska eller internationellt vedertagna normer kan användas som referens (artikel 19.1). Mot bakgrund av de internationella standarder som är fullt utvecklade och som finns på plats på det här området, rekommenderar vi att en certifiering, där lämpliga standarder finns, av en av dem (som till exempel ISO 27001) bör vara tillräcklig för att uppfylla kraven.

- I varje fall bör en standardcertifiering vara frivillig och inte tvingande. Artikel 19 betonar att en standard endast kan ”uppmuntras” och detta bör ske ”utan att ålägga eller särskilja användning av en viss typ av teknik”.

e) Rapportering säkerhetshändelser

- Som vid säkerhetsåtgärder, spelar många parter en roll när det gäller att utforma händelserapporteringen enligt nät- och informationsdirektivet. Medlemsstater måste garantera att digitala tjänsteleverantörer anmäler de säkerhetshändelser som har en betydande inverkan på tillhandahållandet av den tjänst (vilken ligger inom direktivets tillämpningsområde) de tillhandahåller (artikel 16.3); samarbetsgruppen ansvarar för diskussioner om anmälningsmodeller (artikel 11.3 m) och kommissionen för att anta genomförandeakterna (artiklarna 16.8 och 9).

- Igen rekommenderar vi att nationella införlivanden hänskjuter processen till genomförandeakterna, av vilka den genomförandeakt som just ska genomföras avseende anmälan måste antas inom ett år efter att direktivet slutgiltigt godkänts.

- När det gäller vilka typer av händelser som bör rapporteras, åläggs digitala tjänsteleverantörer att meddela ”varje händelse som har en betydande inverkan på tillhandahållandet av tjänsten ” (artikel 16.3). När det gäller implementering av motsvarande bestämmelser för telekomoperatörer enligt artikel 13 a i ramdirektivet, tror vi att detta bör tolkas så att det sker en inriktning på **kontinuitet (eller tillgänglighet)** för de tjänster som tillhandahålls. Med andra ord bör driftsavbrott som uppnår ett visst tröskelvärde (som ska fastställas i genomförandeakterna) rapporteras snarare än någon annan typ av säkerhetshändelse. Detta har fördelen att det sker en fokusering på de händelser som mest sannolikt kommer att påverka ekonomin eller samhället samtidigt som en minimering (även om det inte blir en fullständig eliminering) sker av överlappningen av anmälningskraven avseende drabbade personuppgifter, vilket härrör från den allmänna uppgiftsskyddsförordningen.

- Dessutom anger anmälningsplikten för ”operatörer av nödvändiga tjänster” att dessa operatörer ska anmäla ”händelser som har en betydande inverkan på kontinuiteten hos de nödvändiga tjänster de tillhandahåller” vilket igen har ett tydligt fokus på tjänstens kontinuitet (eller tillgänglighet). Medlagstiftarna har samtyckt till att åliggandena för digitala tjänsteleverantörer bör vara mildare än de som gäller för operatörer av nödvändiga tjänster (se skäl 49). Skyldigheten avseende händelserapportering enligt nät- och informationsdirektivet för digitala tjänsteleverantörer bör inte vara mer omfattande än skyldigheterna för operatörer av nödvändiga tjänster. I själva verket bör skyldigheten vara ännu mer skräddarsydd vad gäller tröskelvärden. Detta belyser ånyo det faktumet att händelserapportering för digitala tjänsteleverantörer bör begränsas till händelser som når en viss

tröskelnivå och **påverkar kontinuiteten/tillgängligheten för tjänster** och inte händelser som rör integritet eller sekretess för data som i en viss utsträckning redan omfattas av relaterade anmälningskrav enligt personskydds- och eIDAS-förordningarna.

- När det gäller tidpunkten för anmälan, uppskattar vi den flexibilitet som antyds genom skrivningen om anmälan. Vi uppskattar den flexibilitet som antyds i ordvalet om anmälan ”utan oskäligt dröjsmål” (artikel 16.3). Implementeringen bör inte leda till stränga tidsfrister då händelser kan variera betydligt vad gäller komplexitet. Enhetliga anmälningstider skulle leda till inkorrekt rapportering när den ursprungliga omfattningen av berörda system är otydlig. Det skulle påverka förmågan hos yrkesmässiga händelserapportörer att prioritera ett åtgärdande av händelsen istället för att anmäla den.

- Som diskuterats ovan kan säkerhetshändelser som ska anmälas enligt direktivet även kräva anmälan enligt dataskyddslagen, beroende på om personuppgifter har drabbats. Inte bara detta innebär rapportering av samma händelser till olika myndigheter, utan myndigheterna kan dessutom finnas i olika medlemsstater beroende på den jurisdiktion som tillämpas för den digitala tjänsteleverantören enligt de två lagarna. Vi rekommenderar att medlemsstaterna erkänner behovet och strävar efter att sörja för en enda händelseanmälan och sträva efter att skapa kommunikationskanaler där relevant information kan delas sinsemellan, utan inverkan på affärssekretessen.

- Behöriga myndigheter bör beakta anseenderelaterade och affärsmässiga följder för digitala tjänsteleverantörer innan information om händelser offentliggörs. Än viktigare är att yppandet av händelsen kan förstärka säkerhetsrisken. Därför är det viktigt att samordna de berörda aktörerna före ett offentliggörande.

- Direktivet understryker att information som betraktas som konfidentiell ska behandlas som sådan (skäl 41, 59, artikel 1.5).

- Artikel 16.3 framhäver att anmälningar om säkerhetshändelser inte ska utsätta den anmälande parten för ökat ansvar.

2. Nödvändiga operatörer

a) Inverkan på säkerhetsåtgärder

- Digitala tjänsteleverantörer som har operatörer av nödvändiga tjänster som kunder, kommer att bli föremål för tillämpliga säkerhetsåtgärder som yttrar sig i avtalsmässiga förhandlingar avseende de nödvändiga operatörernas stadgeenliga skyldigheter (artikel 14.1). De kan i sig indirekt bli föremål för nationell lag i kundernas hemländer, oavsett tillämplig lag där de har sitt europeiska säte.

- Därför torde satsningar på att harmonisera säkerhetsåtgärderna för nödvändiga operatörer vara välkomna. Samtidigt som medlemsstaterna har rätt att ålägga nödvändiga operatörer strängare skyldigheter än de som finns i direktivet (artikel 3), rekommenderar vi en begränsning av detta och uppmuntrar medlemsstaterna att arbeta för en harmoniserad metod. Detta kan uppnås genom att undvika ytterligare åtgärder i nationella införlivanden och genom att sträva efter att fastställa lämpliga säkerhetsåtgärder i samarbetsgruppen istället för att fokusera på den nationella processen.

DIGITALEUROPE
Rue de la Science 14, 1040 Bryssel [Belgien]
Tel: +32 (0) 2 609 53 10 Fax: +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Medlem i kommissionens öppenhetsregister: 64270747023-20

- Säkerhetskraven bör så långt det är möjligt baseras på internationella standarder (som till exempel ISO 27x-serien) och erkänd god säkerhetspraxis.

- De säkerhetsåtgärder som åläggs operatörer av nödvändiga tjänster bör inte i något fall medföra krav på att särskilda IKT-produkter utformas, utvecklas eller tillverkas på ett visst sätt (skäl 51).

b) Påverkan nedåt av rapportering av säkerhetshändelser

- Operatörer av nödvändiga tjänster måste rapportera säkerhetshändelser hos sina kontrakterade digitala tjänsteleverantörer där händelserna påverkat kontinuiteten för deras nödvändiga tjänster (artikel 16.5). Digitala tjänsteleverantörer kommer därför att enligt avtal tvingas rapportera till operatören av nödvändiga tjänster i fråga händelser om kan komma att påverka dem.

- Vi uppskattar flexibiliteten för anmälningstidpunkten för operatörer av nödvändiga tjänster, något som framgår av frasen ”utan oskäligt dröjsmål” (artikel 14.3). Nationella införlivanden bör inte medföra särskilda tidsfrister och om operatörer av nödvändiga tjänster uppmanas att bestyrka den tid en anmälan tar, ska i varje fall den period under vilken de förväntas göra anmälan inledas när operatören blir medveten om händelsen, inte från den tidpunkt när den digitala tjänsteleverantören blir medveten om händelsen.

- Artikel 14.7 förutser att samarbetsgruppen drar upp riktlinjer för omständigheterna avseende anmälan i motsats till kommissionens harmoniseringsroll för anmälningar från digitala tjänsteleverantörer. Mot bakgrund av de dubbla rapporteringskraven för digitala tjänsteleverantörer, är det viktigt att de olika anmälningskraven inte är motstridiga och att de samordnas så mycket som möjligt. Följaktligen bör denna process styras in mot det målet. Dessutom bör anmälningskraven för digitala tjänsteleverantörer följa de sekretesskrav de har gentemot de kunder som utgörs av operatörer av nödvändiga tjänster och inte begära av dem att dela med sig av sekretessbelagd företagsinformation.

DIGITALEUROPE
Rue de la Science 14, 1040 Bryssel [Belgien]
Tel: +32 (0) 2 609 53 10 Fax: +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Medlem i kommissionens öppenhetsregister: 64270747023-20

OM DIGITALEUROPE

DIGITALEUROPE representerar den digital teknikbranschen i Europa. Våra medlemmar inkluderar några av världens största IT-, telekom- och konsumentelektronikföretag och nationella organisationer från varje del av Europa. DIGITALEUROPE vill att europeiska företag och medborgare fullt ut ska dra nytta av de digitala teknikerna och att Europa ska växa, locka till sig och bibehålla världens bästa teknikföretag.

DIGITALEUROPE tryggar branschdeltagande vid utveckling och genomförande av EU:s politik. DIGITALEUROPE:s medlemmar omfattar 62 företagsmedlemmar och 37 nationella branschorganisationer från hela Europa. Webbplatsen innehåller mer information om de senaste nyheterna och vår verksamhet: http://www.digitaleurope.org

DIGITALEUROPE – MEDLEMSKAP

Företagsmedlemmar

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

Nationella branschorganisationer

Belgien: AGORIA
Bulgarien: BAIT
Cypern: CITEA
Danmark: DI Digital, IT-BRANCHEN
Estland: ITL
Finland: FFTI
Frankrike: AFNUM, Force Numérique, Tech in France
Grekland: Sep
Irland: ICT IRELAND
Italien: ANITEC
Litauen: INFOBALT
Nederländerna: Nederland ICT, FIAR
Österrike: IOÖ
Polen: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Rumänien: ANIS, APDETIC
Schweiz: SWICO
Slovakien: ITAS
Slovenien: GZS
Spanien: AMETIC
Storbritannien: techUK
Sverige: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Turkiet: Digital Turkey Platform, ECID
Tyskland: BITKOM, ZVEI
Ukraina: IT UKRAINE
Ungern: IVSZ
Vitryssland: INFOPARK

DIGITALEUROPE
Rue de la Science 14, 1040 Bryssel [Belgien]
Tel: +32 (0) 2 609 53 10 Fax: +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Medlem i kommissionens öppenhetsregister: 64270747023-20